NASA Activities in Risk Assessment

NASA Project Management Conference

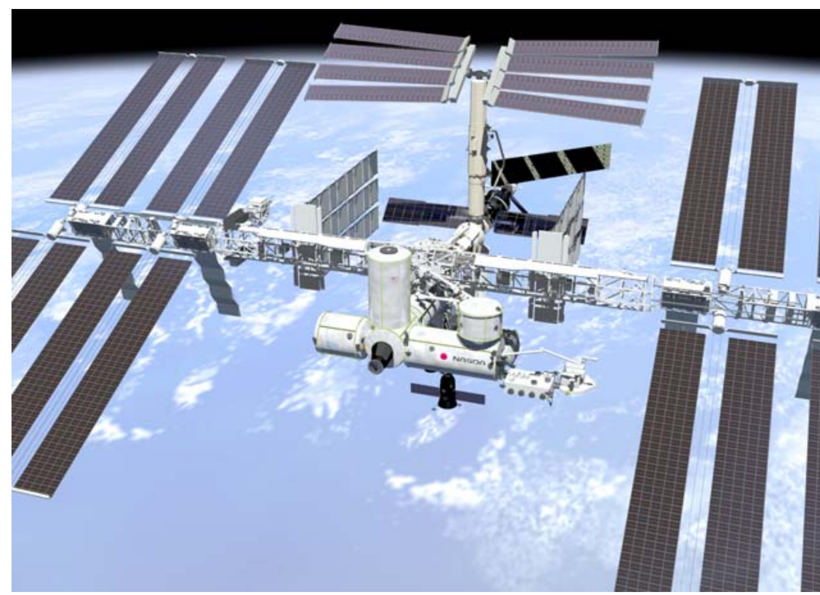
March 30-31, 2004

Michael G. Stamatelatos, Ph.D.,Director
Safety and Assurance Requirements Division
Office of Safety and Mission Assurance
NASA Headquarters

NASA is a Pioneer and a Leader in Space; Therefore Its Business Is Inherently Risky

International Space Station

- Safe assembly and operation



Space Transportation

- Space Shuttle
- Orbital Space Plane

Our Goal

- ***Improve risk awareness in the Agency***
  - *Conduct PRA training for line and project managers and for personnel*
- ***Develop a corps of in-house PRA experts***
- ***Transition PRA from a curiosity object to baseline method for integrated system safety, reliability and risk assessment***
- ***Adopt organization-wide risk informed culture***
  - *PRA to become a way of life for safety and technical performance improvement and for cost reduction*
  - *Implement risk-informed management process*

Probabilistic Risk Assessment (PRA) Answers Three Basic Questions

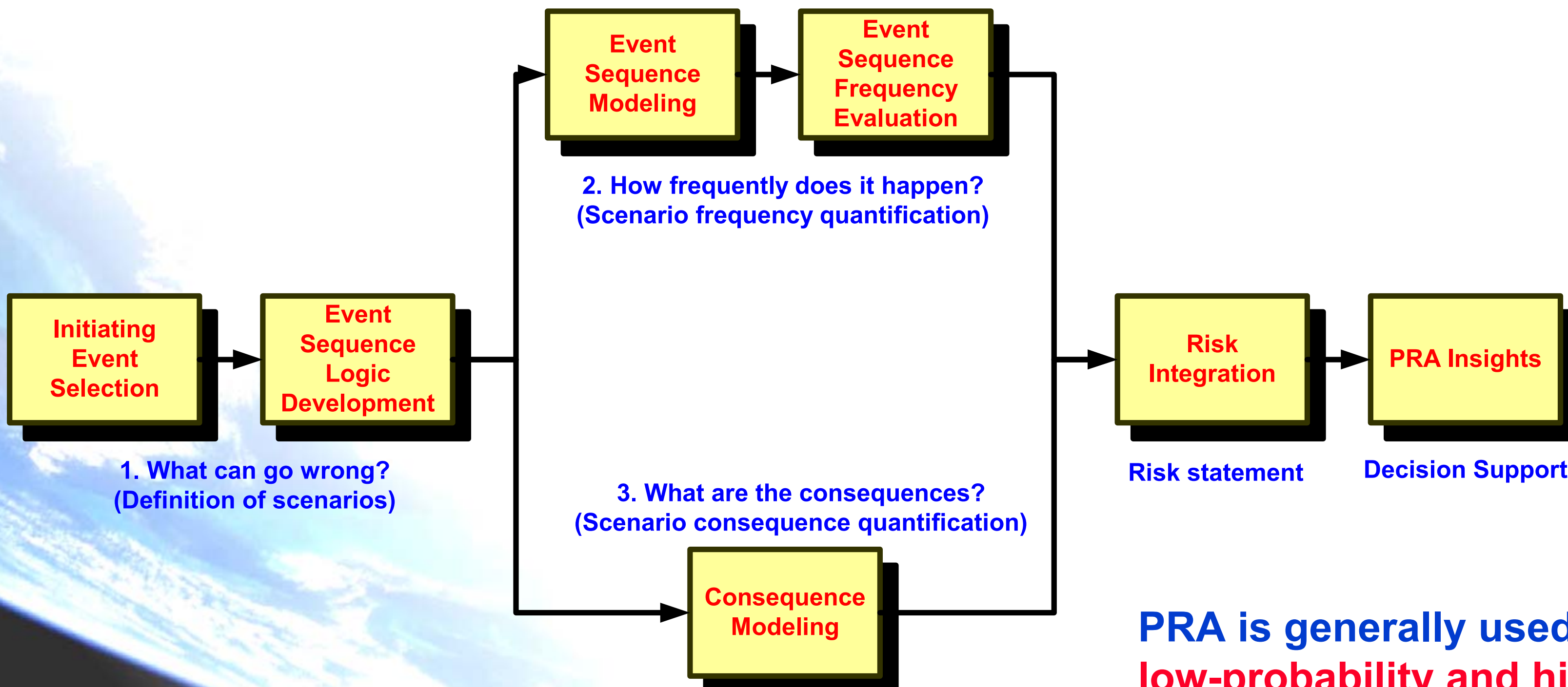
Risk is a set of **triplets** that answer the questions:

1) What can go wrong? (accident **scenarios**)

2) How likely is it? (**probabilities**)

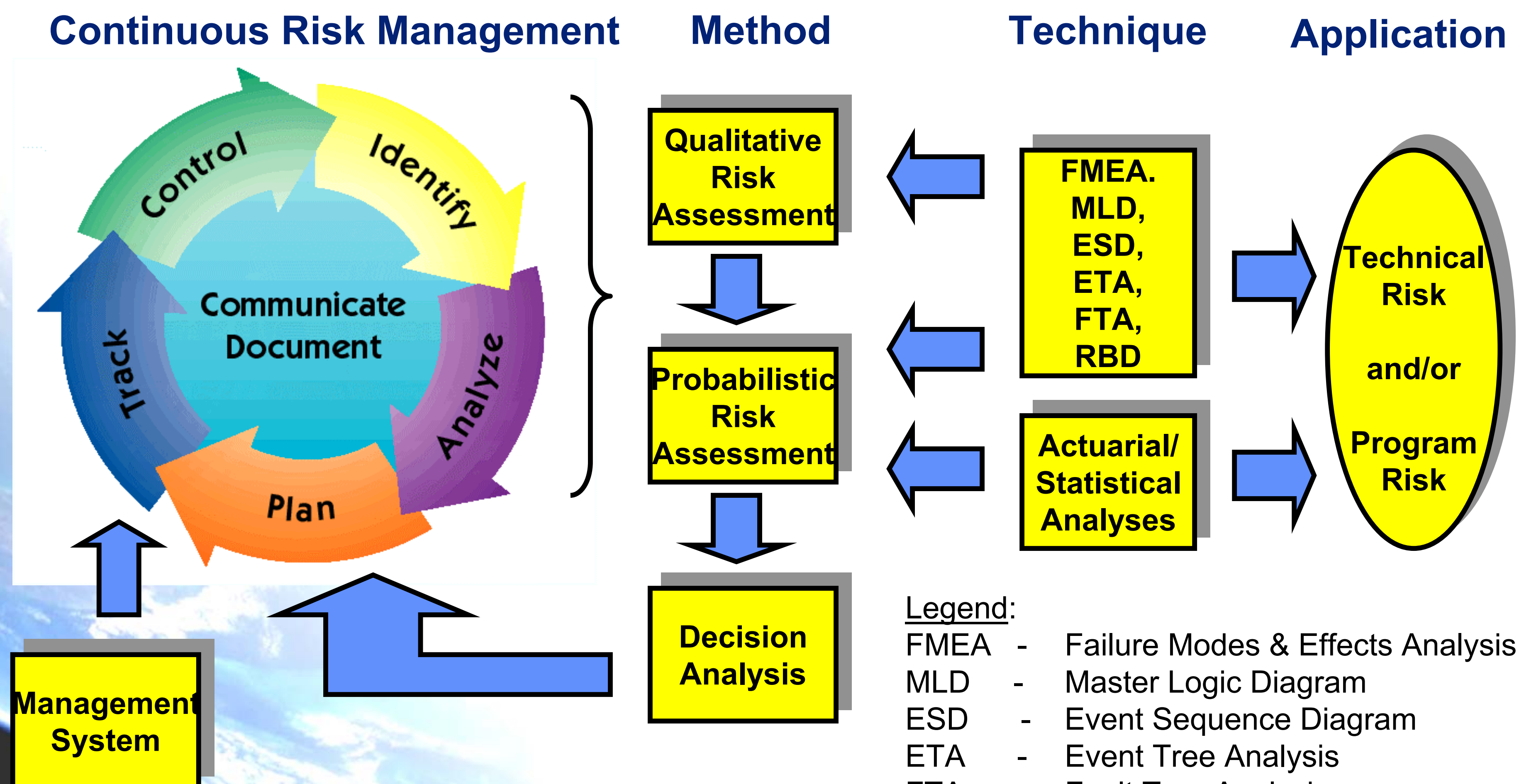
3) What are the **consequences**? (adverse effects)

Kaplan & Garrick, *Risk Analysis,* 1981



PRA is generally used for low-probability and high-consequence events

Relationship Between Risk Management and Probabilistic Risk Assessment (PRA)



Legend:

FMEA - Failure Modes & Effects Analysis
MLD - Master Logic Diagram
ESD - Event Sequence Diagram
ETA - Event Tree Analysis
FTA - Fault Tree Analysis
RBD - Reliability Block Diagram

NASA Risk Management and Assessment Requirements

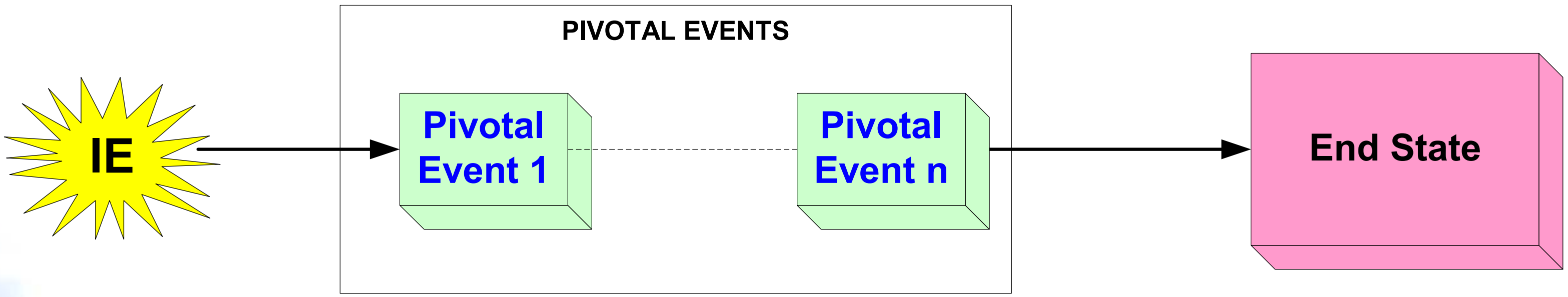
- **NPG 7120.5A, NASA Program and Project Management Processes and Requirements**
  - *The program or project manager shall apply risk management principles as a decision-making tool which enables programmatic and technical success.*
  - *Program and project decisions shall be made on the basis of an orderly risk management effort.*
  - *Risk management includes identification, assessment, mitigation, and disposition of risk throughout the PAPAC (Provide Aerospace Products And Capabilities) process.*
- **NPG 8000.4, Risk Management Procedures and Guidelines**
  - *Provides additional information for applying risk management as required by NPG 7120.5A.*
- **NPG 8705.x (draft) PRA Application Procedures and Guidelines**
  - *Pro*
    progra

How Does PRA Help Safety?

Provides a basis for risk reduction through:

1. ***Accident/Mishap Prevention***
2. ***Accident/Mishap Consequence Mitigation***

The Concept of an Accident Scenario



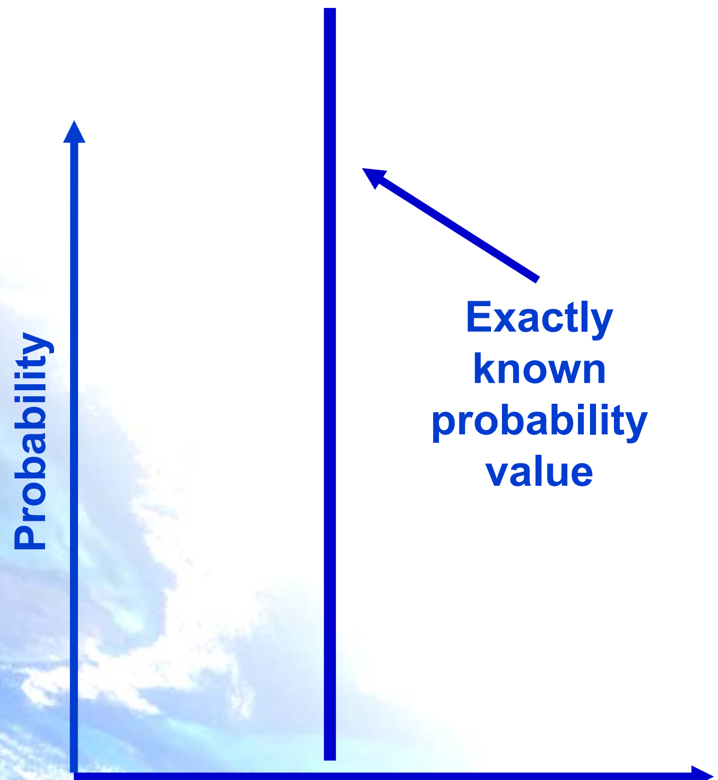
The perturbation

- ❑ Mitigative
- ❑ Aggrevative

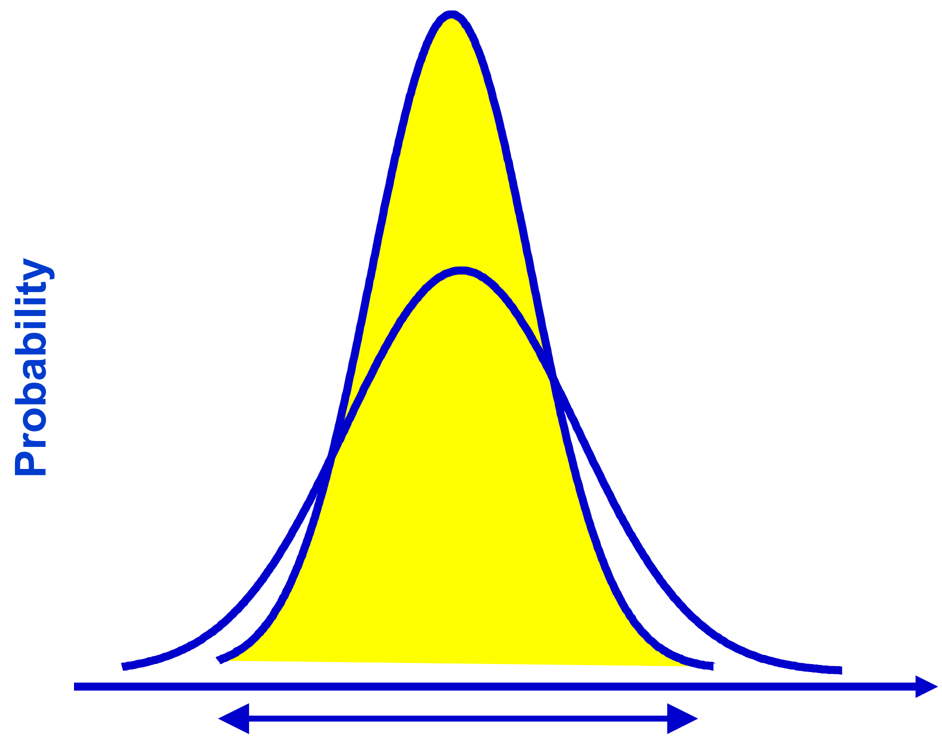
Detrimental consequence of interest
(Quantity of intereset to decision-maker)

Risk Scenario is a string of events that (if they occur) will lead to an undesired end state.

Exact vs. Uncertain Probabilities



Uncertainty distribution
of probability values



A narrower range means a more
precise knowledge of the distribution,
or less uncertainty

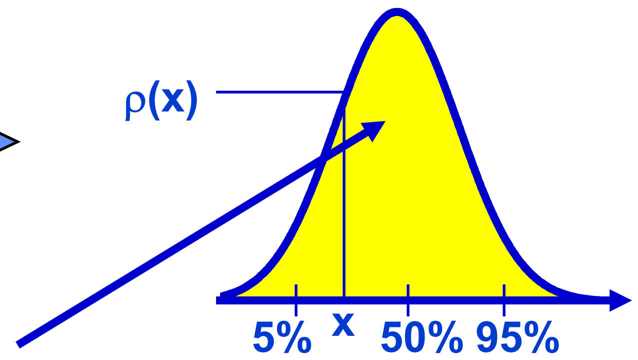
Quantification of Uncertainty

Probability density function,
e.g., probability of LOCV

Uncertainty Distribution:

- *P(x) is the probability (or x^{th} percentile confidence) that the result value is x*
- *median is the 50^{th} percentile*

P(x) is area under curve between 0 and x



Median

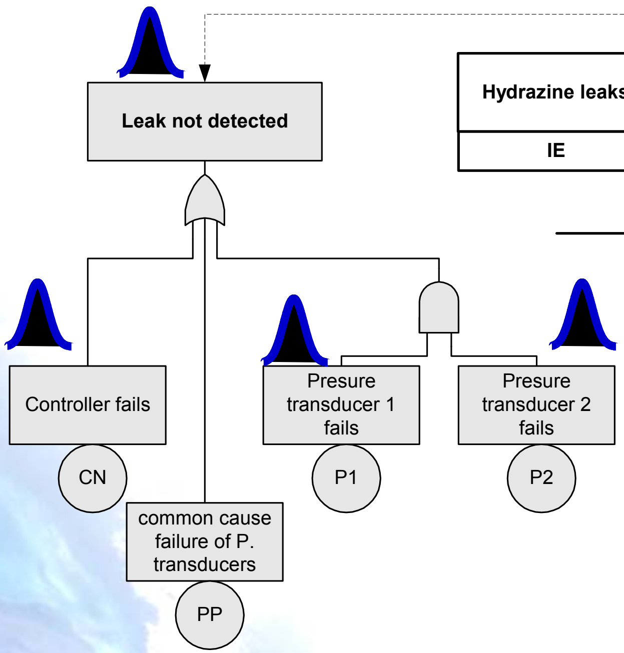
Uncertainty Range:

- *Uncertainty range (spread) from the 5^{th} to the 95^{th} percentile*

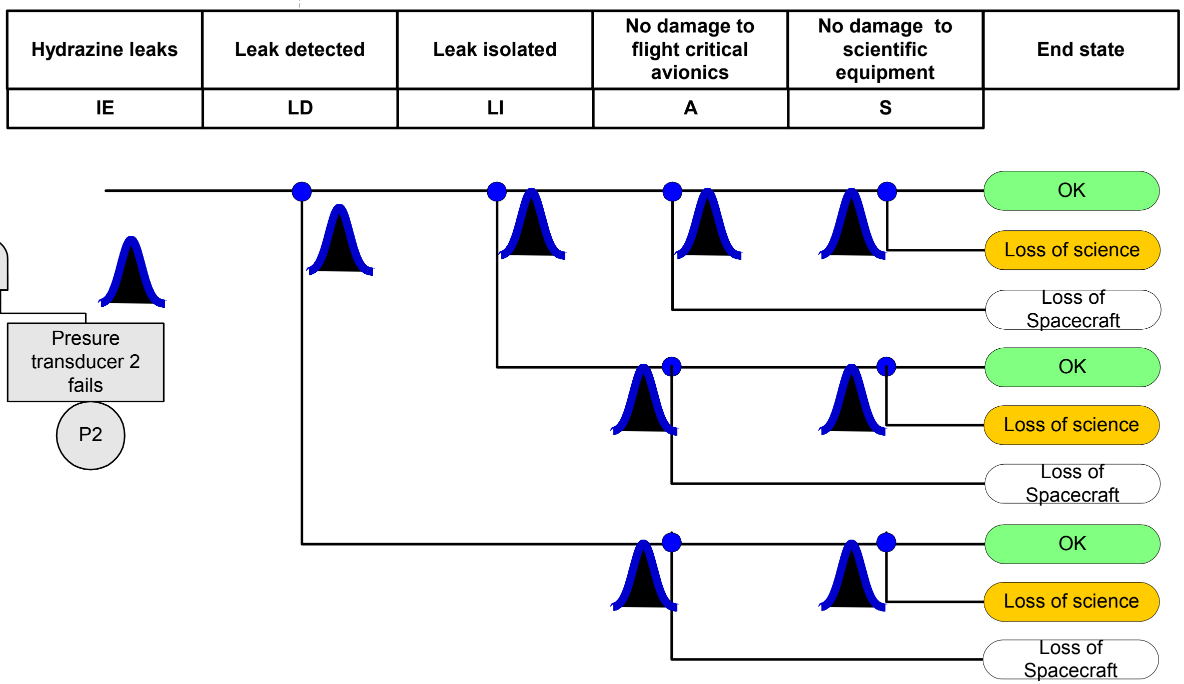
5^{th} percentile **95^{th} percentile**

Uncertainty (confidence) range

Event- and Fault-Tree Scenario Modeling



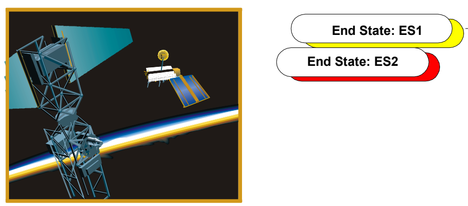
Fault tree



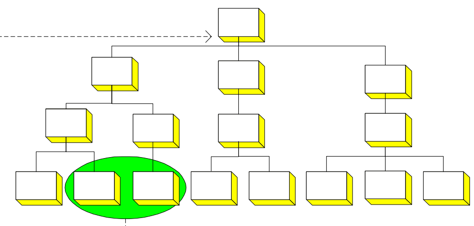
Event tree

PRA Methodology Synopsis

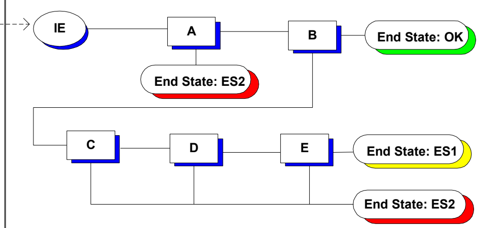
Inputs to Decision Making Process



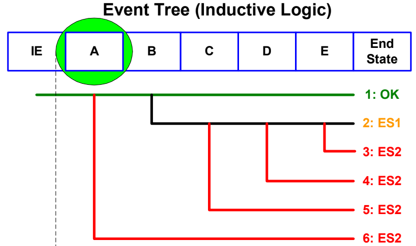
Master Logic Diagram (Hierarchical Logic)



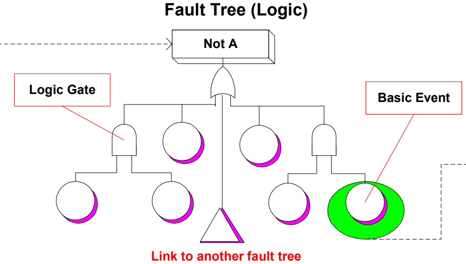
Event Sequence Diagram (Logic)



Event Tree (Inductive Logic)



Fault Tree (Logic)



One to Many Mapping of an ET-defined Scenario

NEW STRUCTURE

- Internal initiating events
- External initiating events
- Hardware components
- Human error
- Software error
- Common cause
- Environmental conditions
- Other

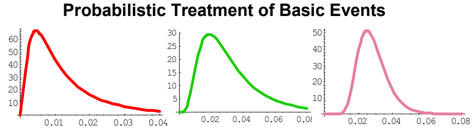
One of these events

AND

one or more of these elementary events

LOGIC MODELING

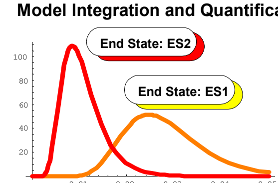
Probabilistic Treatment of Basic Events



Examples (from left to right):
Probability that the hardware x fails when needed
Probability that the crew fail to perform a task
Probability that there would be a windy condition at the time of landing

The uncertainty in occurrence of an event is characterized by a probability distribution

Model Integration and Quantification of Risk Scenarios



Integration and quantification of logic structures (ETs and FTs) and propagation of epistemic uncertainties to obtain

- minimal cutsets (risk scenarios in terms of basic events)
- likelihood of risk scenarios
- uncertainty in the likelihood estimates

Risk Results and Insights

- Displaying the results in tabular and graphical forms
- Ranking of risk scenarios
- Ranking of individual events (e.g., hardware failure, human errors, etc.)
- Insights into how various systems interact
- Tabulation of all the assumptions
- Identification of key parameters that greatly influence the results
- Presenting results of sensitivity studies

PROBABILISTIC

What Decision Types Can PRA Support?

- *Safety improvement in design, operation, maintenance and upgrade (throughout life cycle);*
- *Mission success enhancement;*
- *Performance improvement; and*
- *Cost reduction for design, operation and maintenance*

For all these areas of application, PRA can help:

- **Identify leading risk contributors and their relative values**
- **Indicate priorities for resource allocation**
- **Optimize results for given resource availability**

Areas of PRA Application at NASA

- *In Design and Conceptual Design (e.g., Crew Exploration Vehicle, Mars missions, Project Prometheus)*
- *For Upgrades (Space Shuttle)*
- *For Development/construction/assembly (e.g., International Space Station)*
- *When there are requirements for Safety Compliance (e.g., nuclear missions like Mars '03; Project Prometheus, Mars Sample Return)*

NASA Procedural Requirement NPR 8705
(Draft)

CONSEQUENCE CATEGORY	CRITERIA / SPECIFICS		NASA PROGRAM/PROJECT (Classes and/or Examples)	PRA SCOPE
Human Safety and Health	Public Safety	Planetary Protection Program Requirement	Mars Sample Return Missions	**F**
		White House Approval (PD/NSC-25)	Nuclear Payloads (e.g., Cassini, Ulysses, Mars 2003)	**F**
		Space Missions with Flight Termination Systems	Launch Vehicles	**F**
	Human Space Flight		International Space Station	**F**
			Space Shuttle	**F**
			Orbital Space Plane/Space Launch Initiative	**F**
Mission Success (for non-human rated missions)	High Strategic Importance		Mars Program	**F**
	High Schedule Criticality		Launch Window (e.g., planetary missions)	**F**
	All Other Missions		Earth Science Missions (e.g., EOS, QUICKSCAT)	**L/S**
			Space Science Missions (e.g., SIM, HESSI)	**L/S**
			Technology Demonstration/Validation (e.g., EO-1, Deep Space 1)	**L/S**

F = Full scope; L/S = Limited or Simplified

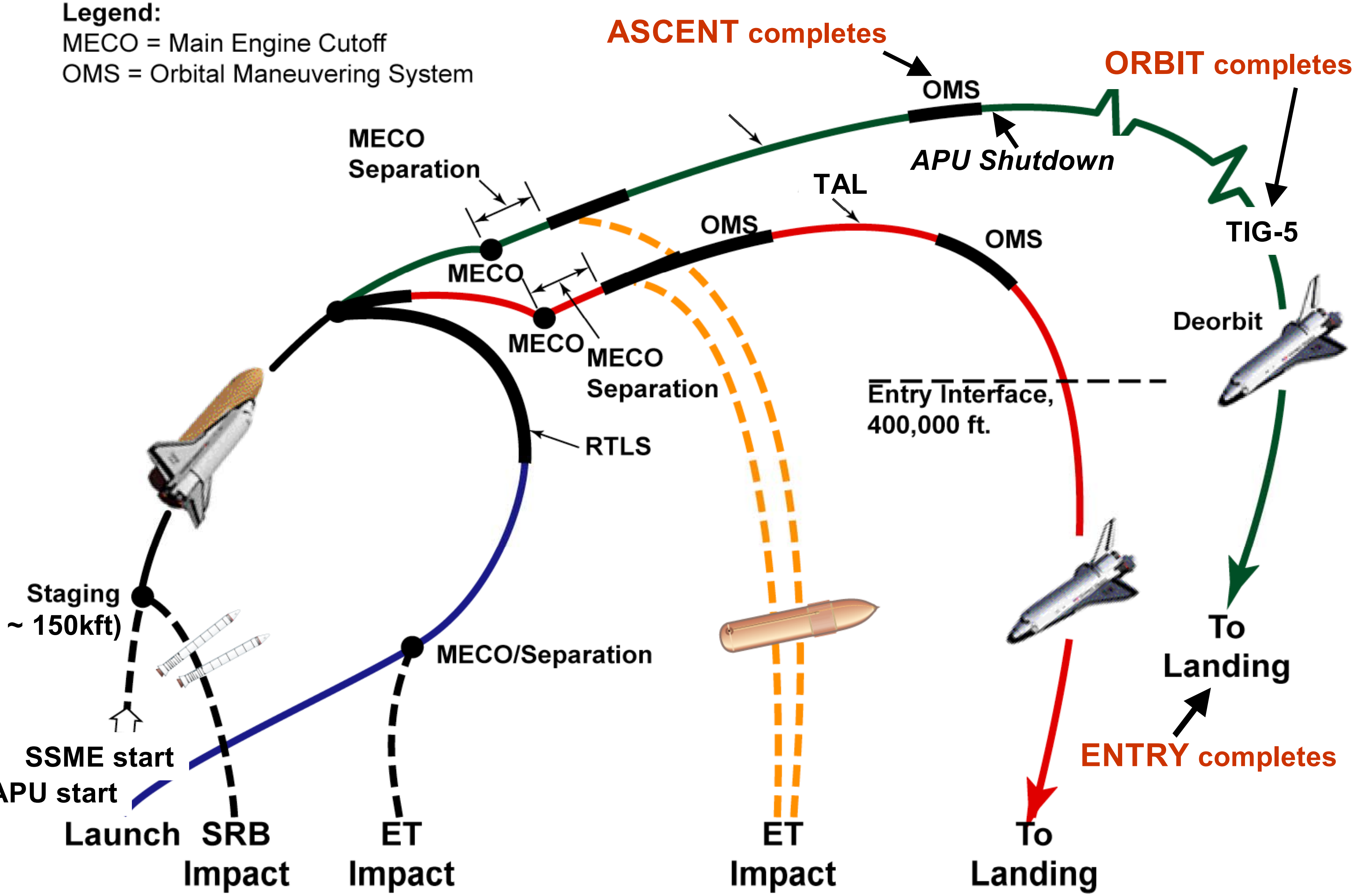
NASA Special PRA Methodology Needs

- *Broad range of programs: Conceptual non-human rated science projects; Multi-stage design and construction of the International Space Station; Upgrades of the Space Shuttle*
- *Risk initiators that vary drastically with type of program*
- *Unique design and operating environments (e.g., microgravity effects on equipment and humans)*
- *Multi-phase approach in some scenario developments*
- *Unique external events (e.g., micro-meteoroids and orbital debris)*
- *Unique types of adverse consequences (e.g., fatigue and illness in space) and associated databases*
- *Different quantitative methods for human reliability (e.g., astronauts vs. other operating personnel)*
- *Quantitative methods for software reliability*

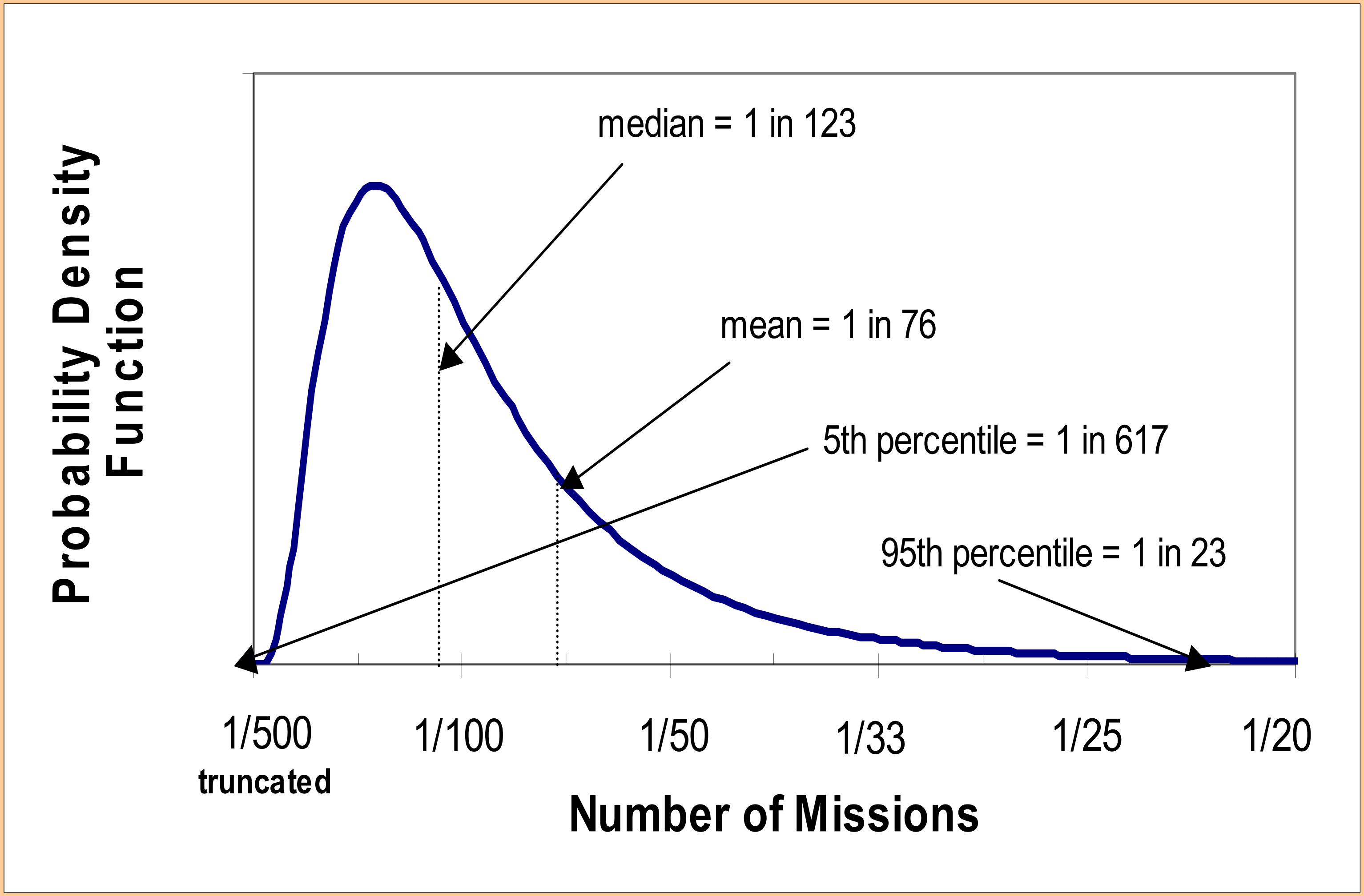
Space Shuttle Probabilistic Risk Assessment

STS Nominal Mission Profile

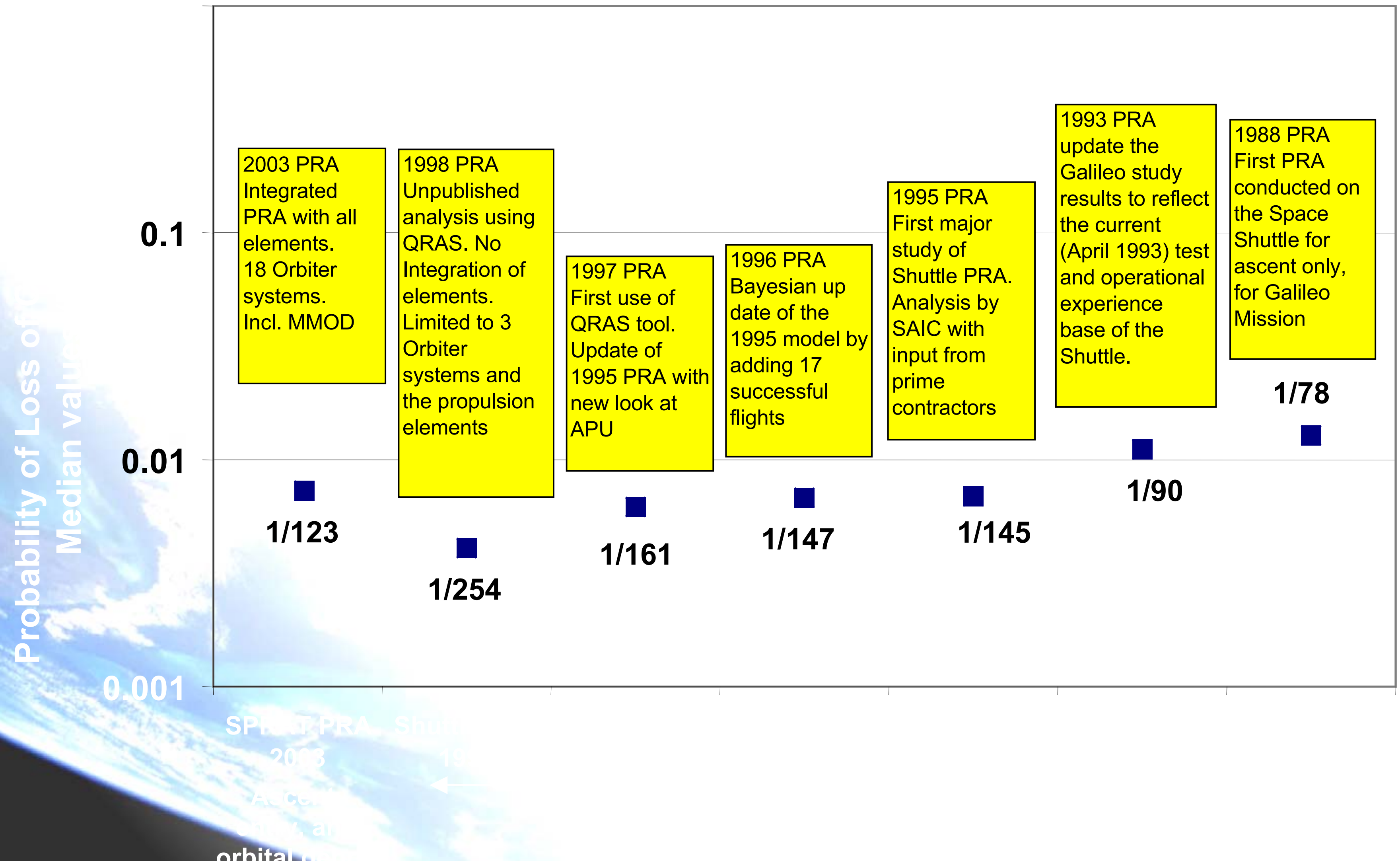
Legend:
MECO = Main Engine Cutoff
OMS = Orbital Maneuvering System



Current Shuttle PRA Results for LOCV
(provisional)



Summary of Shuttle PRA Historical Results



Annual Voluntary Risks in Some Sports - Comparable in Magnitude to Shuttle Risk

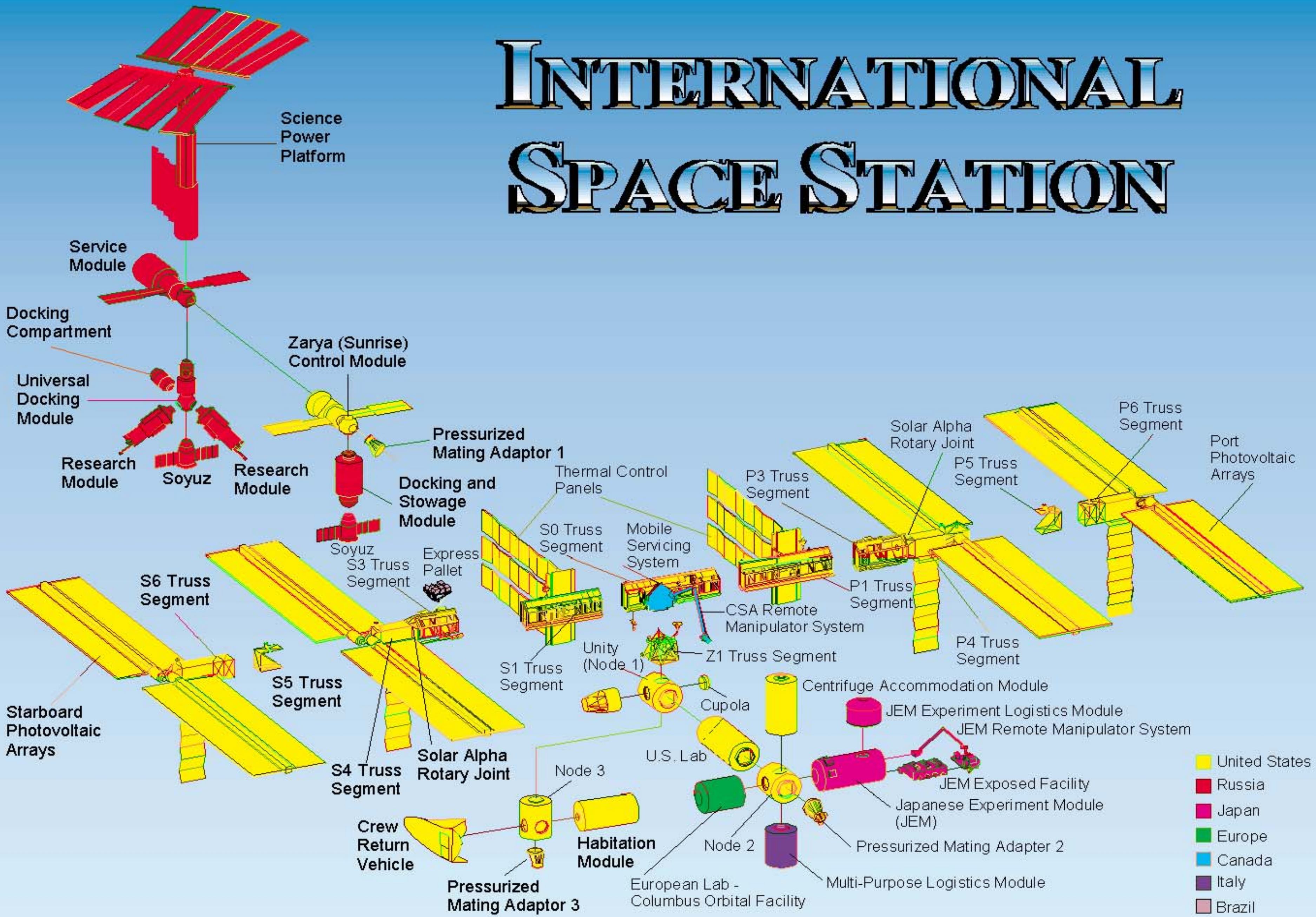
• Professional stunting	1/100
• Dedicated mountain climbing	1/167
• Air show/air racing and acrobatics	1/200
• Amateur flying in home-built aircraft	1/333
• Experienced whitewater boating	1/370
• Sport parachuting	1/500

Source: R. Wilson and E. Crouch, Risk-Benefit Analysis, Harvard University Press, 2001

International Space Station (ISS) PRA

- 1999 -- The NASA Advisory Council recommended, the NASA Administrator concurred, and the ISS Program began a PRA.
  - The modeling will be QRAS-compatible.
  - First portion of PRA (through Flight 7A) - delivered in Dec. 2000; Second portion (through Flight 12A) delivered in July 2001.

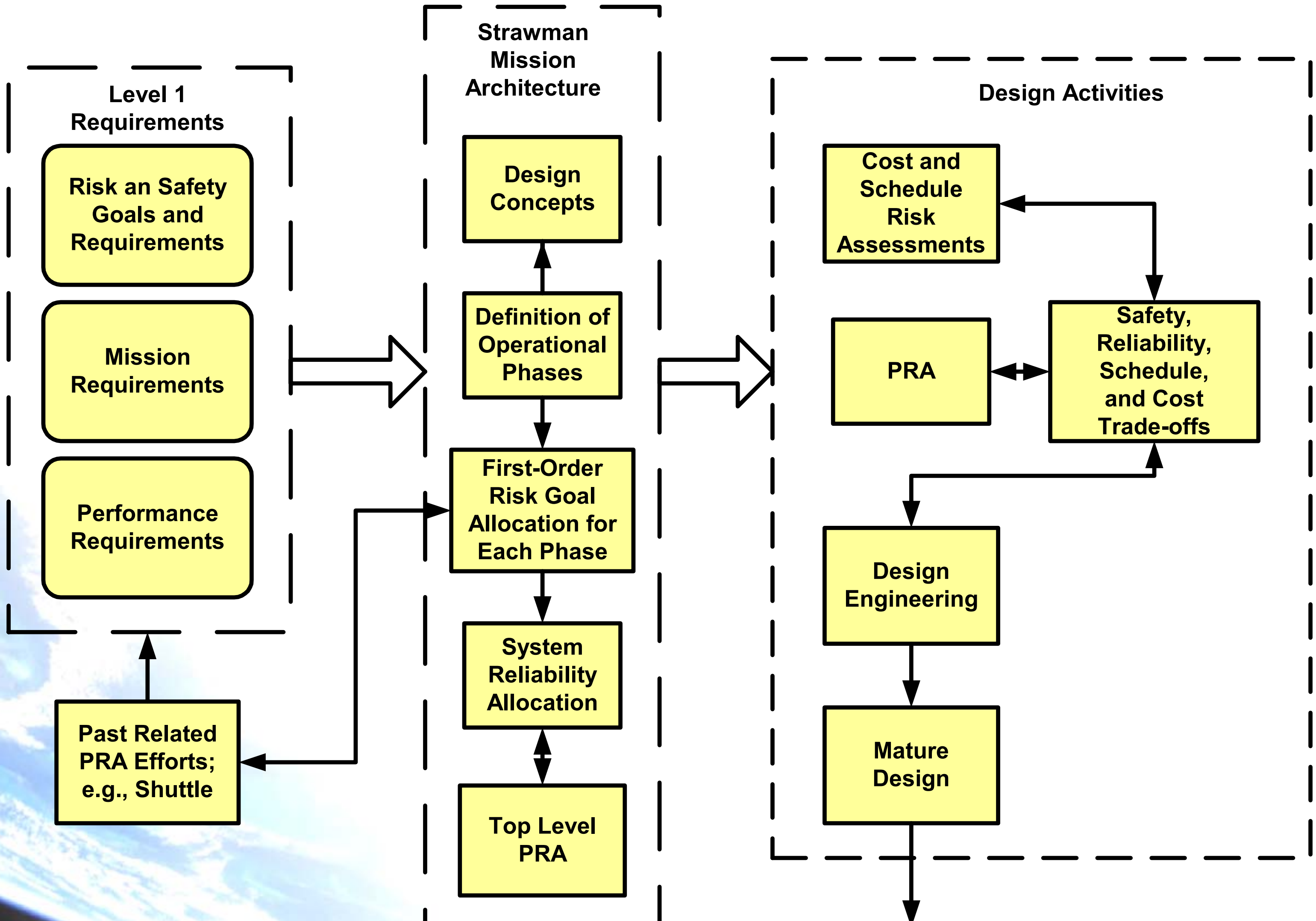
INTERNATIONAL SPACE STATION



Important ISS PRA Findings

- **MMOD**: lead contributor to loss of station (**LOS**) risk
- **Illness in space**: lead contributor to loss of crew (**LOC**) risk

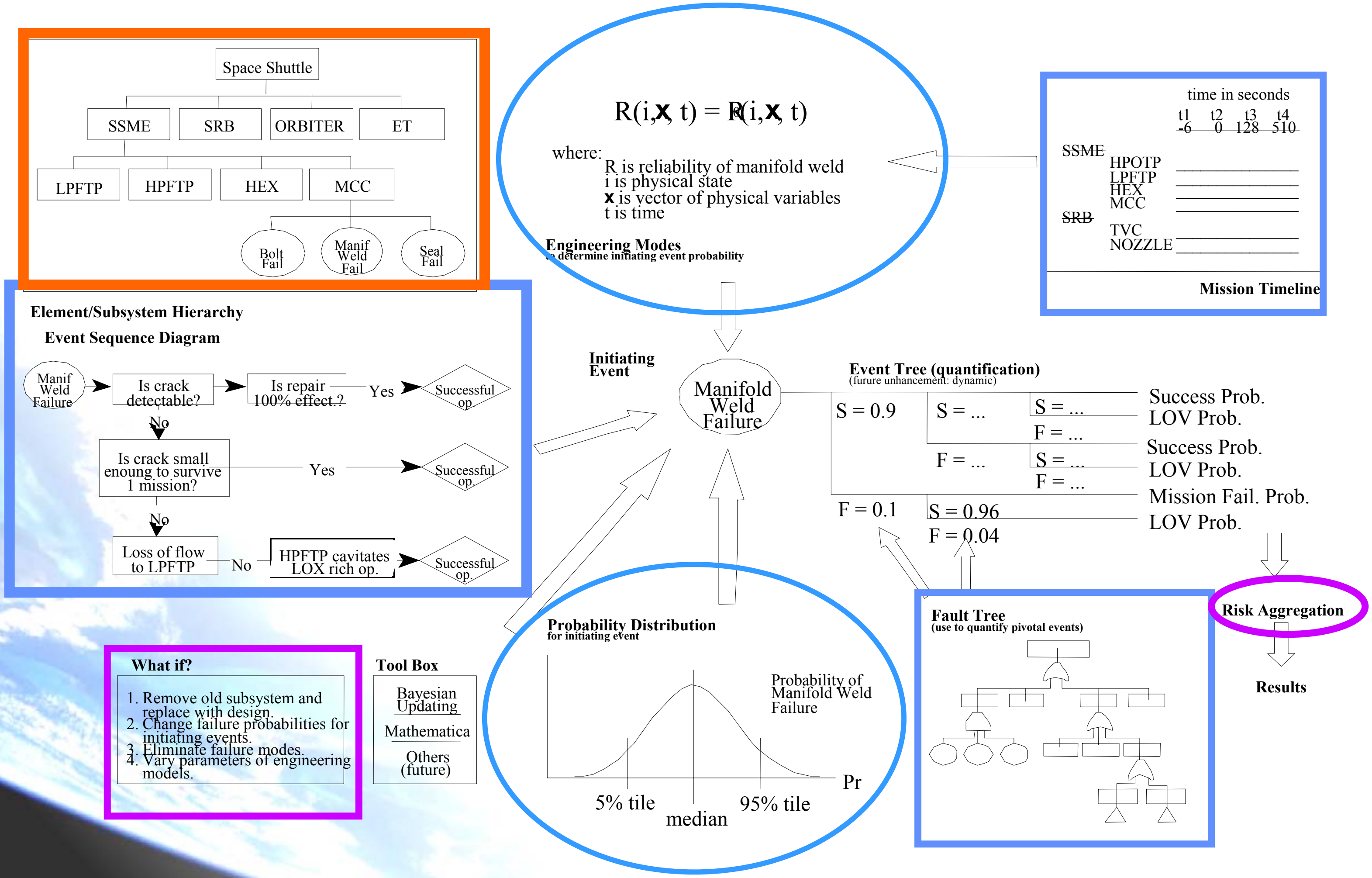
Approach to PRA for NASA Top-Level Designs (e.g., Crew Exploration Vehicle)



Advanced PRA Methods or Tools

- ***QRAS* (Quantitative Risk Assessment System) – a state of the art integrated PRA computer program**
- ***Galileo/ASSAP* – Dynamic fault tree program**
- ***Software reliability* methodology for use in PRA**
- ***External event methodology for micro-meteoroid and orbital debris (MMOD) risk into the overall risk assessment***

QRAS 1.7 Is Being Commercialized



In Summary, We Plan to

- ***Continue to improve risk awareness***
  - *Conduct PRA training for line and project managers and for personnel*
- ***Continue to develop a corps of in-house PRA experts***
- ***Transition PRA to baseline method for safety assessment***
- ***Integrate risk assessment with system safety and reliability assessment***
- ***Adopt organization-wide risk informed culture***
  - *PRA to become a way of life for safety and technical performance improvement and for cost reduction*
  - *Implement risk-informed management process*